Physician PDA Use and the HIPAA Privacy Rule

Paul E. Pancoast, MD, Timothy B. Patrick, PhD, Joyce A. Mitchell, PhD
Health Management and Informatics, University of Missouri-Columbia

Abstract. Physicians need better access to information when making patient care decisions. Hospitals should allow electronic data transfers to physician PDAs to improve patient care, and physicians must institute measures to secure the confidentiality of patient information on their PDAs. By explicitly excluding copies from their designated record set, hospitals need not maintain copies or track access of information on personally owned PDAs.

Introduction. Disruptions in information availability can be a proximate cause in medical errors.[1] However, increased availability of patient information must not jeopardize patient privacy. The Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enforced as of April 14, 2003. This rule protects the confidentiality of all identifiable health information regardless of storage media, but is not intended to restrict the flow of information between providers for treatment purposes. Individuals are given rights with respect to information stored in a designated record set: to request restrictions on use and disclosure, to inspect and copy, to amend or request amendment, and to receive an accounting of disclosures. Each covered entity must appoint a Privacy Officer to develop and implement policies and procedures for protection of confidentiality and to ensure the rights of individuals are maintained, including the right to inspect and copy information in the designated record set.

Scenario. A physician in a group practice attends patients at several hospitals. She downloads new patient data into her PDA at one hospital during rounds and again at a second hospital. Later, during office hours, she receives a call requesting patient orders. After consulting her PDA, she issues the appropriate orders. Her PDA contains data from three different covered entities: two hospitals and her own office practice. Even though there may be conflicts between the policies of the covered entities, she follows the policies of the primary covered entity for whom she works, whether it is a hospital, health plan, or her own practice.

Hospital Concerns. Hospitals have concerns about the confidentiality of information given to physicians. Another concern is the individuals right to inspect, copy, and see who has accessed the designated record set. However, copies of documents provided to physicians may be excluded from the designated record set, and need not be monitored by the hospital.[2]

PDA Security. PDAs may contain large amounts of legible data, including names, federal identifiers, diagnoses, medications, and billing information. Information may be stolen either by physically taking the PDA or by intercepting infra-red (IR) data transmissions in a public location. There are several precautions that should be taken by every health care provider who has patient information on a portable electronic device:

- Maintain careful physical control of the device at all times
- Use data encryption technology
- Power-on password protection
- Disable IR ports except during use
- Don't send IR transmissions in public locations[3]

Conclusion. Hospitals should allow physicians to download patient information into their PDAs to improve patient care decisions. If physicians have patient information in their PDAs, they must assume the responsibility for safeguarding the confidentiality of that information. Physicians' office privacy policies should cover information on PDAs.

Acknowledgements. This research was supported in part by Library of Medicine Biomedical and Health Informatics Research Training grant 2-T15-LM07089-11.

---

1. McKnight L, Stetson PD, Bakken S, Curran C, Cimino JJ. Perceived information needs and communication difficulties of inpatient physicians and nurses. *Proceedings/AMIA Annual Symposium. p.* 2001.

2. NCHICA. Guidance for Identifying Designated Record Sets Under HIPAA. 02/03/2003. Available at: http://nchica.org/HIPAAResources/Samples/Guidance.pdf. Accessed Feb.11, 2003.

3. Blanton SH. Securing PDAs in the Health Care Environment. *SANS Info Sec Reading Room.* 09/06/2001. Available at: http://www.sans.org/rr/pdas/health_care.php. Accessed Feb.16, 2003.